Integrated Intelligent Iter-Itra (ICUBE) Network Box

Inventors: Kannan P. Vairavan

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to the field of computer networking and more particularly to the field of small office home office (SOHO) connecting various computing devices such as wireless AP, Bluetooth, Fiber to the home(FTTH), xDSL, Cable modem, Firewall etc.

2. Description of Background Art

The office networking markets need an integrated, intelligent and long term solution to networking problems that exist today such as those problems described below. What is needed is a system that will not be obsolete and will provide internet and intranet connectivity that is secure and allow for future expansion of the system as new technologies emerge.

For the past 20 years, companies have been purchasing computers, cables and wires with various networking components

that are incompatible. These systems also require expert installers. In addition, networking technologies in the market place have been changing at a rapid pace. This phenomenon creates a need for each office to periodically upgrade their inter or intranet infrastructure. Today there are many alternative ways of providing internet and intranet connectivity. All of this leads to confusion in the market place with respect to xDSL, fiber and wireless connectivity and how these mediums will be integrated within a small office, home office or home environments. The costs of power consumption, rewiring, replacing obsolete components and configuring the network are expensive.

The architecture of the present invention has conceptualized a network device, which addresses the above challenges. With this invention, a goal is to create a new standard for secured network connectivity which allows companies to connect to the internet and intranet by many alternate means, provide inter-operability of all the computers within a small office while increasing the overall cost efficiency and office productivity. The present invention's 'ICUBE box' will network desktop and portable computers, allow communication with xDSL, fiber, or wireless compatibility, and provide a security firewall. This ICUBE box has the added benefit of expandability and 'Evergreen' properties that allows the users to upgrade easily to meet the changing technologies, eliminating obsolescence.

Conventional systems have attempted to solve the above problems. Many boxes are required to connect various computing devices today. Technologies are emerging very rapidly with various standards and some times the inter operability becomes an issue due to proprietary standards. The problems associated with such technology include: (1) they are hard to maintain multiple technology with multiple boxes; (2) they consume more power, space and are more expensive; (3) they are cumbersome to interconnect computers with various boxes.
No adaptation with emerging technology; (4) it is difficult to add and drop computing devices; (5) they require additional cables to interconnect various boxes with computing devices and (6) when an emerging technology is available, the existing one will become obsolete after the new replacement.

SUMMARY OF THE INVENTION

A system and method for connecting various intranet computing devices and internet computing devices in a SOHO environment. The architecture is compatible with past, present and future technology without rewiring and avoids cumbersome wiring. This allows the user to add or drop any intra or inter

computing devices with multiple technology and to easily configure and maintain the system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

A preferred embodiment of the present invention is now described with reference to the figures where like reference numbers indicate identical or functionally similar elements. Also in the figures, the left most digits of each reference number corresponds to the figure in which the reference number is first used.

The present invention is an integrated intelligent Intra-Internet network box, also referred to herein as an "ICUBE box" for small office and home office (SOHO). The ICUBE box is an "Ever-Green Box" designed to expand and support upgrades and new technologies. The various function of the ICUBE box includes the following functionality and advantages:

(a) xDSL card connects to ISPs through existing POTS line. 10/100 base T switch to connect up to nX24 various computing devices with internal IP address.

(b) A secured wireless access point network card to connect between office buildings or to connect wireless devices within a building.

(c) A Fiber To The Home (FTTH) interface card to communicate with external world (ISPs) up to 100 Mb/sec.

(d) A built in firewall & intrusion detection with various feature to protect internal networks from any external viruses or hackers.

(e) A Bluetooth card to control various appliances within a building and communicate with various small bandwidth wireless devices.

(f) All the cards in the box are with plug and play feature. Each card can be replaced by new card based on standard based emerging technology and will be easily configured.

This easy to use evergreen ICUBE box gives the user a feature rich unified solution. Compatibility with past and evolving technology, support of mobility with security make this product unique and cutting edge. The product with this invention will increase productivity by giving users mobility, convenience, flexibility, simplicity, added functionality, compatibility and finally security. This product will integrate all the above mentioned state of the art technology and will provide users with low cost high performance solution.

As Internet usage continues to explode in conjunction with the proliferation of PCs and servers, the race to get broadband devices into the SOHO environment is on at a furious pace. The deployment of services such as xDSL, fiber, Bluetooth, wireless, cable modems, multi-service routers, etc. is continuing at a break-neck speed. The telecom players and the ISPs are beginning to offer multiple broadband services (ATT/@Home) and architecture defined in figure.1 is "Integrated Intelligent Inter-Intra (ICUBE) Network Box" focused on offering a unified solution for multiple broadband services via one device for locations with multiple computing appliances that need to be networked.

ICUBE BOX Architecture

The architecture includes 5 processing components as shown in figure 1, they are

1. System Processor
2. Access Devices
3. Packet Processor
4. Security Processor
5. Switch Fabric

1. System Processor

The system processor is a general-purpose microprocessor. The important functions of the system processor are to configure all the components to function properly, co-ordinate and supervise all the activities of the board and communicate with external world either through ISP or through other computing devices by using GUI interface. The system processor has a capability to upgrade necessary software and various tables of all the components from time to time to maintain evergreen concept. It also coordinates with packet processor to generate logging information for various purposes such as intrusion detection and statistics. Certain protocols needed by the switch fabric will typically be provided by the system processor. The system processor will provide GUI interface that is easy to navigate.

- GUI interface will be used to manage the entire system, on a per box basis, centrally, from a local site or remote site, from which different types of information will be made accessible with enforceable access privilege to configure, monitor and change the system.
- GUI interface can have an SNMP client to generate SNMP requests from the user directly.

- System events can be logged and stored, analyzed and reports will be generated (automatic) that can be sent to the administrator, and critical events can be highlighted.
- Copies of all the tables and critical data generated by the Packet Processor can be stored and forwarded to the administrator.
- Port access can be controlled, configured or blocked by the administrator as needed for the level of security of the network.

2. Access Devices

All devices connected to packet processor bus are called access devices. Access device includes xDSL board, FTTH, Cable Modem, Wireless Access Point, Wireless ISP, etc. These access devices are to communicate with outside building. The architecture accommodates multiple devices with different technology or with same technology for higher throughput.

The packet processor receives and transmits data to and from access devices. These devices can be hot pluggable and play. If any one of the access devices becomes outdated with respect to technology, the device can be replaced by a newer technology

device without disturbing any physical connections since the architecture supports the evergreen concept. All the access devices are to be designed in such a way to be compatible with the packet processor bus in order to communicate.

3. Packet Processor

The Packet Processor gets data to and from the following processing components.

1. Access Devices
2. Security Processor
3. System Processor
4. Switch Fabric

Upon receipt of a packet, the processor needs to perform firewall & intrusion detection functionality, routing, VPN & NAT analysis, IPSec function, etc. Packet Processor with the computational help from the system processor will device various security policies and tables.

Information Management

Information (tables) that should be modeled and stored in the database: Information consists of policy data, user data, configuration data and service data.

Enterprise Customer Data

Examples include: Customer name, customer id, services (software functionalities such as Intrusion Detection etc) the customer subscribed to be stored in this table. Information in this table will be used by software to invoke appropriate software functionalities.

VPN Site

A VPN table contains information about individual sites of an enterprise. There is one entry for each site and site id is the key. Examples include: site id, location, IP address of the box, id of the central site, identifying information of the box such as its product number, software version number of that box, number and list of SAs from that site to every other site, number and list of SAs from that site to the central site.

For multi-site, one way of maintaining the VPN is as follows: All traffic destined for an enterprise terminates on the head office box. IP Packet may or may not be IPSEC encapsulated. If it is IPSEC encapsulated, the following action is taken by the router: it is decrypted and the inner IP packet is checked for the destination address. If the destination address is in another branch, it is encapsulated in another IPSEC envelope and sent to the other branch via the already established VPN tunnel. If the destination is in the same branch, it is routed appropriately. If the incoming IP packet is not IPSEC encapsulated, and if it is destined for a remote site, it is encapsulated in an VPSEC envelope and sent there. The IP address of the destination in the IPSEC envelope is the IP address of the remote box. Remote boxes work as follows: when traffic terminates on those boxes, they take the same action as the head office box except that the traffic is always destined for nodes within the remote box.

Evergreen box configuration information

The site number should be used to index this table and it contains should contain information about the individual evergreen box of that site. For example: product number, IP address of the box, software version number, number of stacked switches in the box, switch identifier/product number of each

switch, IP address of the Bluetooth Access Point, ESSID (Extended Service Set) of the 802.11 access point, IP address of the IEEE 802.11 access point, number of VLANs.

LAN configuration information & Table generation

This table has information about the LAN configuration of a site and the site number should be used to index it. For wired equipment, it might contain switch number, port number, equipment number (MAC address), and IP address of the equipment, network services, if any, provided by the equipment. For wireless equipment, it might contain MAC address of the equipment (for Bluetooth equipments, it is the 48-bit IEEE 802 Bluetooth device address), IP address of the equipment. It could also include the VLAN number. If Network Intrusion Detection is enabled, it should list of ports/hosts to be monitored.

Network Address Translation (NAT)

The NAT table should contain one entry for each network device in the enterprise. The entries should map the local IP address and local TU (TCP/UDP) port into Globally registered IP address and assigned TU port number. Each entry should contain the site id to indicate where the device is located. This

information is useful when more than one global IP address is assigned to a site as well as when an internal address is reused in another site. Each site holds entries correspond to devices located in that site along with global addresses of every site. Central site (System Processor) should have the complete table.

Since all traffic in/out of a site goes through the same packet processor of the box in that site, this translation, when done by the packet processor, should not cause any problem. The Packet Processor of the box serves as the NAT router. Assignment of private to public address can be done when a host initiates a session, and the mapping for the private id should be retained for subsequent sessions.

Port Table for inbound sessions

This table should contain port information that is needed for inbound sessions such as DNS lookup. The table, for example, should contain site id, box id, network service name, box IP address, and assigned port number for that service.

User Information Tables

This table should contain information such as:

1. User id.

2. User access privilege

3. User name

4. Password (encrypted)

5. Host(s)

6. VLANs for which the user has access to

7. A list of services accessible to the user

8. Whether or not the user is a mobile user

9. Public key (if any)

10. Corresponding encrypted private key

11. Last time the user logged on to the system.

Security Policy for firewall

The system for specifying packet-filtering rules based on the source and destination address found in layer 3 Ipv4 or Ipv6 packet header. The table contains the source IP address, source TCP/UDP port number, destination IP address, and the destination UDP/TCP port number.

Some of the rules that can be used for packet filtering are:

1. Drop all source-routed packets.

2. If incoming packet claims to be from local net, drop it.

3. All packets, which are part of already established TCP-connections, can pass through without further checking.

4. Allow all outgoing TCP-connections

5. Allow incoming SMTP and DNS to mail host

Table of Open Security Associations & Associated Information (SAD)

The table of currently open Security Associations, along with the associated information (SAD), defines the parameters associated with one SA. Each SA has an entry in the SAD.

A table entry should have the following types of fields:

1. Sequence number for AH or ESP header

2. Sequence counter overflow (a flag to indicate if overflow should prevent further transmission on that SA)

3. Anti-replay window (used to determine if a packet is a replay)

4. AH authentication algorithms and keys

5. ESP Encryption algorithm, keys

6. ESP Authentication algorithm and keys

7. Lifetime of this Security Association (time interval)

8. IPSEC protocol mode (tunnel, transport, wildcard), Initialization Vector (IV)

9. Path MTU

IPSEC Processing (Security Policy Database)

Table to maintain security policy information for IPSEC Processing Table (Security Policy Database).

This table should describe what services are to be offered for IP data grams and in what order. SPD requires distinct entries for inbound and outbound traffic.

Each selector entry may include:

1. If IPSEC processing is to be applied to the traffic, bypassed or the packet has to be discarded.
2. If IPSEC processing is to be applied, the entry includes SA specification, IPSEC protocols, modes, and algorithms to be employed including any nesting requirements.
3. The policy entry includes specification of the derivation of Security Association Database (SAD) entry, from the SPD entry and the packet. This may be to direct the user to use the value in the packet itself or the value associated with the policy entry.
4. The parameters that must be supported for SA management are Destination IP address (can be range of addresses as well as wildcard address), Source IP address, Name (user id or system name; can be opaque), transport layer protocol (can be

opaque), source and destination TCP/UDP ports (can be wild card or opaque).

THE FIREWALL COMPONENT

The Firewall component provides NAT (network address translation) function to map incoming IP addresses to local IP addresses of the VPN, Identification and authentication and Access control.

Firewall lets us specify who can access what functionalities in the VPN. Access rules can be specified via the GUI interface. Access control can be specified to the granular level of files or objects, and can be grouped together to form one entity to apply a policy for a group for ease of management.

The firewall will provide:

- Intrusion Detection and alert functions (email/network advisory/etc.)
- User and group specific network logging and management
- Content Filtering
- Packet Filtering
- Stateful Packet Inspection
- Network Anti-virus management [Future enhancement]

- Port protection/blocking/configuration (completely customizable)

Network Intrusion Detection Mechanism

Network intrusion detection system monitors traffic (IP packets) to/from a reselected (configured by the system administrator) set of machines. Intrusion detection mechanism will be based on anomaly detection and misuse detection. Anomaly detection identifies variation in usage pattern against a pre-established baseline usage pattern. This includes identifying usage pattern anomaly in number of log-ins, file access, CPU utilization. Misuse detection looks for predefined known attack patterns in the traffic.

Content Filtering

Content filtering can be applied in two ways:

1. By specific IP address.
2. By URL name

A table can be used to match an IP address or URL and deny the user access before leaving the protection of the firewall. Likewise, if an IP is used and an authorized URL is returned, the

firewall will deny the access on the inbound. The same rule can be applied to the for a URL not listed, but returning an unauthorized IP address.

Stateful Packet Inspection

As part of complete protection, the box will be able to interrogate packets to identify the states the packet has completed (e.g. ACK)

Network Anti-virus management

The box shall provide an anti-virus update agent that will monitor connected PC's and provide automatic updating of a partnered anti-virus package.

Port protection/blocking/configuration

Port access can be controlled, configured or blocked by the administrator as needed for the level of security of the network.

4. Security Processor

The security processor provides IPSec (3DES) functionality and work very closely with packet processor. IPSec provides a standard for encryption of other wise un-secure IP packets. It does this by providing a standard architecture to use, including two new protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides proof-of-data origin on received packets, data integrity, and anti-replay protection. ESP provides everything that AH provides plus optional data confidentiality and limited traffic flow confidentiality.

In order to encapsulate and de-capsulate IPSec packets another protocol, Internet Key Exchange (IKE), is implemented to negotiate keys and establish and manage a Security Association (SA). The processor does IPSEC algorithms for encryption, decryption, and authentication in terms of digital signature. The Packet processor does invocation of them with appropriate parameters and packet.

Switch Fabric

Switching offers a high level of performance and speed for the nodes being switched with-in a close area-link or similar type technology. Wide area links and differential technologies are more aptly handled by the routing function.

The switch shall provide 2 one gigabit ports and N* 10/100 ports. One gigabit port shall be used for communication to the packet processor, while the other will be made available for addition of another switch fabric component, which will allow another N* 10/100 physical Ethernet ports to be connected to the box.

The Switch contains a routing table and helps to do the following:

a) The routing table must be configurable to be static or dynamic.

b) The routing table must be configurable (display and edit).

c) The routing table must allow for a configurable default entry.

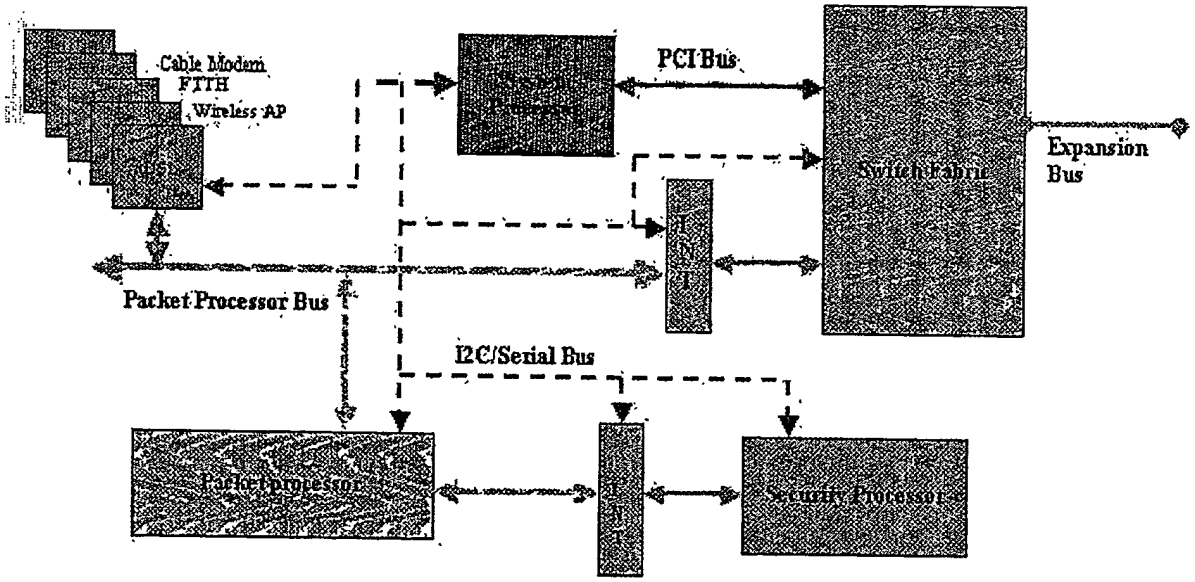
d) The routing table must adhere to defaults set by the Routing Function.

e) The Switch must support Ipv4 & Ipv6.

f) The switch shall report any configuration and self-test errors.

Inter-site Communication

For multi-sited enterprises, communication mechanism will be established so that different sites can communicate with each other. Initially, when the system is started, tunnels have to be established between every pair of sites (a mesh structure) that would facilitate nodes/hosts within each site to communicate with other nodes/hosts in other sites. The inter-site communication link will be established by a wireless (IEEE 802.11) access device.



Sooriya's Evergreen Icube Box Architecture

Knann P Vairavan

5. Physical Box Architecture

The chassis will be made of three different parts, bottom, top and front bezel. 24 Ethernet ports, and 2 Giga ports will face to the front. Eight of the Ethernet modules will be connected through the backside. A USB port will be connected to the backside.

Chassis will have a rack mount optional kit that will include side ears, and/or side rails (depends upon the weight of the box). Length of the box will be a standard rack mount size, depth will be guided by the size of the PCB/electrical circuit (7"-10") and height will be guided by the height of the highest plug in module. At present it looks like it will be 18"x 10"x 2U. 1U is 1.75".

Power supply will be module type and will be mounted to the bottom of the chassis along the right side (looking from front) with a detachable power cord. An EMI Filter/fuse/switch will be mounted to the backside of the chassis and it will connect detachable AC cord to the power supply module.

A cooling fan will be placed for air circulation. Size, type (AC or DC) and position of fan have not been determined yet.

More likely the fan position will be 2/3 to the back on the right side, close to the power supply.

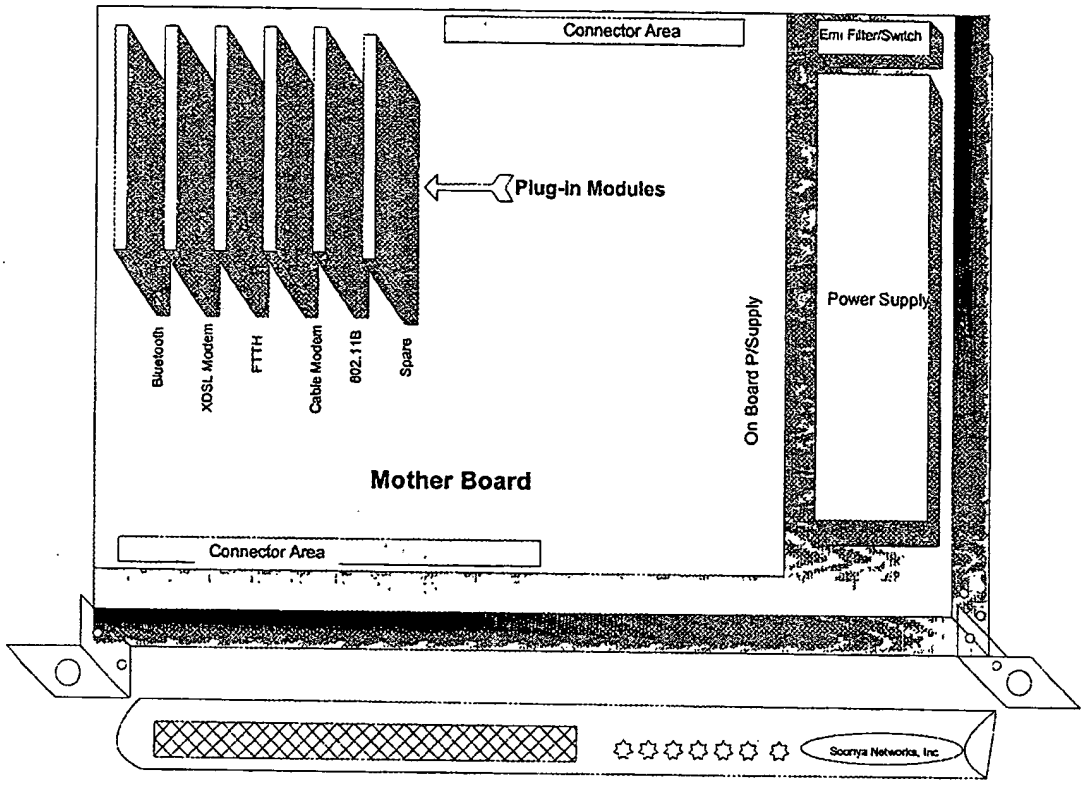


Figure 2, The Physical Box Layout (Chassis)

6. Advantages

There are many unique features and differentiators that separate ICUBE box from conventional systems including:

1. It can operate as a stand-alone networking device to connect all the SOHO appliances in a wired or wireless environment that is secure. This enables the sharing of the resources such as printers and files amongst the many appliances such as desk-tops and lap-tops.

2. Any form of broadband access can be utilized and shared including all the flavors of DSL, cable, wireless and fiber applications.

3. A firewall and intrusion detection are included to isolate the SOHO appliances from the external broadband networks.

4. Bluetooth functionality is provided to monitor the SOHO appliances.

5. Adjacent buildings of an office can be networked together in a wireless medium, thereby, sharing common broadband modem resources. For example, employees in three different buildings can share the ADSL service terminated by the carrier in one of the buildings providing economies.

6. Customized interfaces can be developed and easily deployed in the box to address to the needs of specific niche markets. An example of this application is the streaming video or entertainment content distribution.

7. The ICUBE box can be managed and administered locally or remotely through the rich array of software hooks provided.

8. Emerging standards in broadband will be supported in a plug and play manner.

9. Secure transmission of data will be provided in the wireless 802.11 environment for within the premise as well as intra-building transmission

Some definitions and acronyms are: (a) SOHO - Small Office/ Home Office; (b) DF - Design Function; (c) MF - Marketing Function; (d) DSL - Digital Subscriber Line; (e) VPN -Virtual Private Network; (f) DNS - Dynamic Name Server (g) SNMP - Simple Network Management Protocol; (h) IPSEC - Internet Protocol Security; (i) LAN - Local Area Network; (j) VPSEC - Virtual Private Security; (k) RIP - Routing Information Protocol; (l) Hello - A Routing Internal Gateway Protocol (IGP) (m) GGP - Gate to Gate Protocol; (n) ICMP - Internet Control Message Protocol; (o) BGP -Boarder Gateway Protocol; (p) OSPF - Open Shortest Path First; (q) SA - Security Authentication; (r) CA - Certificate Authority; and (s) VLAN - Virtual Local Area Network.

While the invention has been particularly shown and described with reference to a preferred embodiment and several alternate embodiments, it will be understood by persons skilled in the relevant art that various changes in form and details can be made therein without departing from the spirit and scope of the invention.